

Topics:

[Mobility \[2\]](#), [BYOD \[3\]](#)  
**Wireless and Mobile Computing [1]**

SS-08-039 Wireless and Mobile Computing

Issue Date: 3/31/2008

Effective Date: 3/31/2008

**PURPOSE**

Wireless and mobile computing technologies offer network users benefits such as portability, flexibility and increased productivity. As employees connect remotely to the state networks, these entry points and data transmission modes increase the risks and vulnerabilities to agency internal networks and must be properly secured.

This standard establishes the minimum requirements for implementing wireless network access.

**STANDARD**

Prior to implementing wireless and mobile technologies, agencies shall be aware of the technical and security implications associated with these technologies and assess the risks to ensure appropriate steps are taken to mitigate these risks.

To mitigate the security risks associated with wireless and mobile computing, system owners shall protect the internal systems by implementing the strongest, most appropriate security controls for encryption, user authentication and end-point protection mechanisms. Anti-virus protection and perimeter controls shall be properly configured and port openings shall be secured, restricted and monitored.

Agencies shall create a Wireless LAN (WLAN) Implementation Plan (as described in the WLAN Implementation Guideline) that adequately addresses the following areas of concern:

- Remote access, wireless access, and mobile computing policies and procedures
- WLAN architecture and implementation
- Configuration and security of access points
- Encryption and encryption keys
- Integration of wireless network to wired network (VPN)
- Security of data transmissions between wired and wireless networks
- Logical and physical protection of wireless/mobile/end-point devices
- Logical and physical protection of stored data in transit.
- Change management and configuration control
- Audit/monitoring
- Penetration tests and vulnerability assessments
- Malicious code protection and Incident handling
- Security Awareness and Training

Agencies shall conduct periodic reviews to ensure that the wireless network and remote access technologies are utilized in a secure manner and in compliance with all applicable security requirements and standards.

The deployment and operation of open, unsecured wireless network access technology is prohibited.